UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,521	08/01/2003	Kim Cameron	MS1-1553US	4349

22971 7590 06/04/2007

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
TIMBLIN, ROBERT M	
ART UNIT	**PAPER NUMBER**
2167	

NOTIFICATION DATE	DELIVERY MODE
06/04/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com
a-rydore@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	10/632,521	CAMERON ET AL.	
	Examiner	Art Unit	
	Robert M. Timblin	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 15-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 15-85* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to application 10/632521 filed on 8/1/03.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/14/2007 has been entered.

Response to Amendment

Claims 1, 53, 61, 65, 74, and 80 have been examined and are pending. Accordingly, claims 1-11 and 15-85 are pending.

Claim Objections

Claim 65 is objected to for the minor informality: it should read "an identity integration system..."(emphasis added).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 80 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, the Examiner finds it confusing as to whether to interpret claim 80 as a system claim or as a method claim. It is vague and unclear as to which statutory category Applicant is claiming.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 53 and accordingly its depending claims are rejected under 35 U.S.C. 101 because claim 53 is directed towards functional descriptive material per se (i.e. a web application is software per se) without being employed as a computer component to impart functionality. When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases. See MPEP 2106.01.

Similarly, claim 61 and accordingly its depending claims are rejected under 35 U.S.C. 101 because they are interpreted to be software per se. Specifically, an interface as defined in Applicant's specification at page 5 line 4-7 defines an interface as an API, which is construed as software. As claim 61 is interpreted to be a manufacture claim, and is a computer related invention, it is construed to be software

per se not recorded on a computer readable medium to impart functionality. Refer to MPEP 2106.01.

Similarly claim 74 and accordingly its depending claims are rejected under 35 U.S.C. 101 because they are interpreted to be software per se. Similar for the reasons of the rejection of claim 53 and 61, a management agent is interpreted as software per se. As claim 74 is interpreted to be a manufacture claim, and is a computer related invention, it is construed to be software per se not recorded on a computer readable medium to impart functionality. Refer to MPEP 2106.01.

Claim 83 is rejected under 35 U.S.C. 101 because it intends to claim a carrier wave and/or data signal (support found on page 55 lines 6-15) which is not statutory under 35 U.S.C. 101. Specifically, a carrier wave and/or data signal are nonstatutory natural phenomenon. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter. MPEP 2106 states:

> While abstract ideas, natural phenomena, and laws of nature are not eligible for patenting, methods and products employing abstract ideas, natural phenomena, and laws of nature to perform a real-world function may well be. In evaluating whether a claim meets the requirements of section 101, the claim must be considered as a whole to determine whether it is for a particular application of an abstract idea, natural phenomenon, or law of nature, and not for the abstract idea, natural phenomenon, or law of nature itself.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20, 22-26, 28-48, 50-52, 54, 58, 60, 62-64, 66, 68-79, and 81-84 are rejected under 35 U.S.C. 102(e) as being anticipated by Hu et al. ('Hu', hereinafter) (US 2004/0158746 A1).

With respect to claim 1, Hu teaches A method, comprising: selecting multiple data sources connected to an identity integration system (page 4, paragraph 0038) wherein:

the identity integration system (Figure 1 and [0033]) includes a management agent (124, 118, 108, 0032, and 0035) for each of the multiple data sources (112, 114, 117) configured specifically for its respective data source [0032] to manage data communication (110) between the identity integration system (figure 1) and each respective data source (112, 114, 117);

for at least some of the multiple data sources (112, 114, 117) a management agent for the data source is configured with credentials to perform password

management as the password management module can be programmed to identify the user [0033]; and

for at least one of the multiple data sources (112, 114, 117) a management agent (124, 118, 108) for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source (a user specifying particular target computers for log-in processing and password access; [0037];

performing a password operation on a password associated with each of the selected multiple data sources, wherein the password operation is performed using the identity integration system (0037, page 4, paragraph 0038, and 0067).

With respect to claim 2, Hu teaches, 'determining an identity of a user, wherein the multiple data sources are associated with the identity' (page 4, paragraph 0038).

querying the identity integration system to find the multiple data sources associated with the identity' (page 4, paragraph 0038).

With respect to claim 3, Hu teaches 'wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system' (page 8, paragraph 0067).

With respect to claim 4, Hu teaches 'the multiple passwords are updated to new passwords that differ from each other' (page 8, paragraph 0067).

With respect to claim 5, Hu teaches 'each of the multiple passwords is updated to the same password' (page 8, paragraph 0067).

With respect to claim 6, Hu teaches 'password operation comprises one of changing, setting and resetting the password' (page 8, paragraph 0067).

With respect to claim 7, Hu teaches 'each of the multiple data sources differ from others of the multiple data sources with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage' (page 3, paragraph 0032).

With respect to claim 8, Hu teaches 'each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage' (page 3, paragraph 0032).

With respect to claim 9, Hu teaches 'each of the multiple data sources uses a different password management function' (pages 2-3, paragraph 0028).

With respect to claim 10, Hu teaches 'the identity integration system performs password management for each of the multiple data sources' (pages 2-3, paragraph 0028).

With respect to claim 11, Hu teaches some of the multiple data sources the identity integration system stores integrated identity information to perform password management (paragraph 0040 and figure 7a).

With respect to claim 16, Hu teaches allowing access to the identity integration system through a web application for password management (page 3, paragraph 0029).

With respect to claim 17, Hu teaches the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application (page 3, paragraph 0029).

With respect to claim 18, Hu teaches the web application accepts a password credential from a user to perform the password operation (page 5, paragraph 0050 and figure 4a).

With respect to claim 19, Hu teaches asking the user questions, wherein if answers provided by the user are correct then the web application performs the

password operation using the identity of a privileged user account (page 2-3, paragraph 0028).

With respect to claim 20, Hu teaches a list of user accounts displayable on the website, wherein the user accounts are associated with the multiple data sources (paragraph 0040 and figure 7a).

With respect to claim 22, Hu teaches communicatively coupling the identity integration system with the web application using an interface (page 3, paragraph 0029).

With respect to claim 23, Hu teaches the interface is publicly available (page 3, paragraph 0029).

With respect to claim 24, Hu teaches interface allows a web application designer to customize the web application (page 3, paragraph 0033).

With respect to claim 25, Hu teaches the interface includes password management functions (page 6, paragraph 0052, and figure 4b).

With respect to claim 26, Hu teaches interface is capable of being changed for an improved version of the interface that adds more password management functions while

using the same web application and the same identity integration system (page 3, paragraph 0033).

With respect to claim 28, Hu teaches the interface is secured using a security group (page 2, paragraph 0027).

With respect to claim 29, Hu teaches interface is secured using a security group that allows both searching for a connector object associated with a data source and setting a password for an object in the data source, wherein a connector object represents at least part of the data source in the identity integration system (page 4, paragraph 0038)

With respect to claim 30, Hu teaches identity of a user associated with the multiple data sources provides a security credential for performing a password operation (page 5, paragraph 0050 and figure 4a).

With respect to claim 31, Hu teaches the web application produces a list of accounts associated with a user (paragraphs 0040, 0071 and figures 5 and 7a).

With respect to claim 32, Hu teaches the web application lists only accounts eligible for password management (page 4, paragraph 0040).

With respect to claim 33, Hu teaches the web application adopts a web application behavior based on a configuration setting (page 3, paragraph 0033).

With respect to claim 34, Hu teaches configuration setting is stored in a configuration file (page 3, paragraph 0033).

With respect to claim 35, Hu teaches the web application checks if one of the data sources is communicating before updating a password associated with the data source (pages 2-3, paragraph 0028).

With respect to claim 36, Hu teaches the updating comprises one of changing and setting the password (page 7 paragraph 0067).

With respect to claim 37, Hu teaches the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source.

With respect to claim 38, Hu teaches the updating comprises one of changing and setting the password (page 7 paragraph 0067).

With respect to claim 39, Hu teaches displaying a status for the password operation (page 6, paragraph 0052, and figure 4b).

With respect to claim 40, Hu teaches displaying the status on a webpage (page 6, paragraph 0052, and figure 4b).

With respect to claim 41, Hu teaches auditing the password operation (page 3, paragraph 0035).

With respect to claims 42 and 71, Hu teaches maintaining a password management history for the password operation (page 0040 and figure 7a).

With respect to claim 43, Hu teaches keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system (page 0040 and figure 7a).

With respect to claim 44, Hu teaches the password management history includes a tracking identifier to an audit record of the password operation (figure 7a and paragraph 0035).

With respect to claim 45, Hu teaches maintaining a repository of audit records for password operations performed using the identity integration system (page 3, paragraph 0035 and figure 7a).

With respect to claim 46, Hu teaches an audit record for a password operation includes at least one of an identifier of a user associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time (page 4, paragraph 0040 and figure 7a).

With respect to claim 50, Hu teaches custom logic performs a password operation on a subsequent data source not connected to the identity integration system (page 3, paragraph 0050).

With respect to claim 51, Hu teaches the password operation further comprises updating passwords in both secure and non-secure data sources within the multiple data sources (page 7, paragraph 0067).

With respect to claim 52, Hu teaches the password operation further comprises updating passwords over both secure and non-secure connections to the multiple data sources (page 2, paragraph 0027).

With respect to claim 54, Hu teaches the identity integration system connects with diverse data sources, each data source having a different function for using password security (page 3, paragraph 0032).

With respect to claim 58, Hu teaches a configuration reader to obtain behavior settings for the web application (page 3, paragraph 0036).

With respect to claim 60, Hu teaches the account lister lists only accounts eligible for password management (page 4, paragraph 0040, and figure 7a).

With respect to claim 62, Hu teaches logic for checking security of a connection between the identity integration system and a data source (page 2, paragraph 0027).

With respect to claim 63, Hu teaches logic to change a password associated with the data source (page 7 paragraph 0067).

With respect to claim 64, Hu teaches logic to set a password associated with the data source (page 7 paragraph 0067).

With respect to claim 66, Hu teaches password management web application verifies one of an identity and a credential of a user (page 5, paragraph 0050 and figure 4a).

With respect to claim 68, Hu teaches the web application operates in a security context (page 4, paragraph 0038).

With respect to claim 69, Hu teaches the security context is an application pool identity (page 4, paragraph 0038).

With respect to claim 70, Hu teaches a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application (pages 7-8 and paragraphs 66-69).

With respect to claim 72, Hu teaches the identity integration system communicates with diverse accounts, each account having a different mechanism for administering a password associated with the account (page 1, paragraph 0006, and page 3, paragraph 0032).

With respect to claim 73, Hu teaches the identity integration system does not natively communicate with at least some of the diverse accounts (page 1, paragraph 0006, and page 3, paragraph 0032).

With respect to claim 74, Hu teaches a management agent for an identity integration system, comprising:

logic for adapting a connection for data communication, wherein the connection couples an identity integration system using a first data communication format with a connected data source using a second data communication format (page 3, paragraph 29, and figure 1).

custom logic configured as code, from a custom logic source outside of the identity integration system, to perform password management for the data source [0037].

logic for requesting a connected data source to perform a password operation (page 3, paragraph 0032).

With respect to claim 75, Hu teaches the management agent performs the password operation (page 3, paragraph 0032).

With respect to claim 76, Hu teaches the management agent requests authorization for performing a password operation (page 3, paragraph 0032).

With respect to claim 77, Hu teaches the management agent is configured with credentials to perform a password management operation (page 3, paragraph 0032).

With respect to claim 78, Hu teaches the management agent is configured with credentials to request a password management operation (page 3, paragraph 0032).

With respect to claim 79, Hu teaches logic to perform a call out for custom logic for performing a custom password operation (page 3, paragraph 0032).

With respect to claim 81, Hu teaches allowing input of user credentials to verify an identity of the user (page 5, paragraph 0050 and figures 4a-4b).

With respect to claim 82, this claim has essentially the same subject matter as set forth in claim 1 above. Therefore, claim 82 is rejected for the same reasons as claim 1 under Hu as set forth above.

With respect to claim 83, Hu teaches multiple data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (page 1 paragraph 0006 and page 3, paragraph 0032).

With respect to claim 84, Hu teaches the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (page 7, paragraph 0067).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 21, 47-49, 53, 55-57, 59, 61, 65, 67, 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hu as applied to claims 1-20, 22-26, 28-48, 50-52, 54, 58, 60, 62-64, 66, 68-79, and 81-84 above in view of Bush et al. ('Bush' hereinafter) (US 2002/0083012 A1).

With respect to claim 21, Hu fails to teach a help desk to at least assist in the performing a password operation.

Bush, however, teaches a help desk to at least assist in the performing a password operation as a password may be sent by telephone to the user (page 2, paragraph 0024).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with a system to send a password to a user (page 2, paragraph 0024, Bush).

With respect to claims 47 and 59, Hu fails to teach the custom logic is executed after the password operation is performed.

Bush, however, teaches the custom logic is executed after the password operation is performed as after the user receives a password, the user enters the password, and access is authorized (page 2, paragraph 0024).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with an account management system to authorize access to the resource (page 2, paragraph 0022, Bush).

With respect to claim 48, Hu fails to teach the custom logic sends an email.

Bush, however, teaches the custom logic sends an email as the password may be sent through an electronic mail message (page 2, paragraph 0024).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with sending a password to the user (page 2, paragraph 0024, Bush).

With respect to claim 49, Hu fails to teach the custom logic logs password management activity.

Bush, however, teaches the custom logic logs password management activity as a connection request is received, it is logged and then completes (page 6, paragraph 0036).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provide Hu's system with a technique that would combine the advantages of a logon organization (page 1, paragraph 0004, Bush)

With respect to claim 53, Hu teaches the amended limitations of this claim as seen in claim 1 as they are substantially similar. Further, Hu teaches a web application for password management, comprising: a user identifier to find user identity information in an identity integration system (page 8, paragraph 0074).

identity information query logic to search information in the identity integration system for accounts associated with the user (page 8, paragraph 0074).

an account lister to display the accounts associated with the user (paragraph 0040, and figure 7a).

a password manager to request an update of a password associated with each designated account to the new password (0028 and page 7, paragraph 0067).

Hu fails to expressly teach an account selector to designate at least some of the displayed accounts for password management and a password inputter to determine a new password.

Bush, however, teaches an account selector to designate at least some of the displayed accounts for password management as an account selection area (page 2, paragraph 0024) and a password inputter to determine a new password (figure 1b).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teachings of Bush would have provided Hu's system with display pages provided by the account management system (page 2, paragraph 0024, Bush) to provide advantages of a logon organization (end of 0004, Bush).

With respect to claim 55, Hu fails to teach an account status display to show selected accounts and a connection status of each account.

Bush, however, teaches an account status display to show selected accounts and a connection status of each account as an indication that the node is currently connected to the server computer (page 3, paragraph 0026, and figure 3).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with an indication for each node currently connected (page 3, paragraph 0026, Bush).

With respect to claim 56, Hu fails to teach a password management operation status for each account.

Bush, however, teaches a password management operation status for each account as an indication that the node is currently connected to the server computer (page 3, paragraph 0026 and figure 3).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with an indication for each node currently connected (page 3, paragraph 0026, Bush).

With respect to claim 57, Hu fails to teach a status checker to verify connectivity and security of a connection between an account and the identity integration system.

Bush, however, teaches a status checker to verify connectivity and security of a connection between an account and the identity integration system (page 3, paragraph 0026, Bush).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with an indication for each node currently connected (page 3, paragraph 0026, Bush).

With respect to claim 61, Hu teaches the limitations as set forth in claim 1 because they are substantially similar in subject matter. Further, Hu teaches an interface for coupling an identity integration system with a password management web application, comprising:

logic for communicating with the identity integration system, wherein the identity integration system is capable of updating a password on data sources that use various functions of password updating (page 7 paragraph 0067).

logic for communicating with the password management web application (page 8 paragraph 0069).

logic for searching for objects in the identity integration system (page 8, paragraph 0074).

Hu fails to teach logic for checking a connection status between the identity integration system and a data source.

Bush, however, teaches logic for checking a connection status between the identity integration system and a data source (page 3, paragraph 0026 and figure 3).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Bush would have provided Hu's system with an indication for each node currently connected (page 3, paragraph 0026, Bush).

With respect to claim 65, Hu teaches the amended limitations as set forth in claim 1 because they are substantially similar in subject matter. Further, Hu teaches a password management system, comprising:

a identity integration system having a metaverse space for persisting integrated identity information regarding accounts associated with a user (page 3, paragraph 0034, and figure numbers 120, 124).

connector space for persisting information representing multiple data sources connectable to the identity integration system (page 2 paragraph 0027 and , and figure numbers 113, 115, 117)

the accounts each corresponding to one of the multiple data sources and having associated manageable passwords (page 1, paragraph 0005-0006 and figure 7a).

an interface to communicatively couple the identity integration system with the web application (page 7, paragraph 0064).

Hu fails to teach a web application for producing a list of the accounts from the identity integration system, for allowing selection of at least some of the accounts, for inputting a password, and for requesting the identity integration system to update passwords on the accounts based on the input password.

Bush, however, teaches

a web application for producing a list of the accounts from the identity integration system for allowing selection of at least some of the accounts (page 2, paragraph 0024, and figure 1a).

for inputting a password (page 2, paragraph 0024, and figures 1a-1b).

for requesting the identity integration system to update passwords on the accounts based on the input password (page 3, paragraph 0024 in respect to fig 1b).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teachings of Bush would have provided Hu's system with displays associated with the logon of users (page 1, paragraph 0004).

With respect to claim 67, Hu fails to teach a webpage that displays accounts and a status of a password management operation for each account displayed.

Bush, however, teaches a webpage that displays accounts and a status of a password management operation for each account displayed (page 3, paragraph 026, and figures 1c and 3).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teachings of Bush would have provided Hu's system with displays associated with the logon of users (page 1, paragraph 0004).

With respect to claim 80, this claim has essentially the same subject matter as claim 65 as set forth above. Therefore, claim 80 is rejected equally for the same reasons as set forth above.

Claims 27 and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hu/Bush as applied to claims 21, 47-49, 53, 55-57, 59, 61, 65, 67, 80 above in view of Davis et al. ('Davis' hereinafter) (US 6,976,262 B1).

With respect to claim 27, the combination of Hu/Bush fails to teach the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface.

Davis, however, teaches the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface as using a WBEM system (col. 4, lines 52-62).

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references

because the teaching of Davis would have provided the combination of Hu/Bush's system with a standard for managing systems, networks, users, and applications by using Internet technology (col. 1 lines 40-50, Davis).

With respect to claim 85, the combination of Hu/Bush fails to teach the identity integration system accomplishes a password update on at least one of an ACTIVE DIRECTORY data source, a SUN ONE server data source, a LOTUS NOTES server data source, a WINDOWS NT server data source, a NOVELL EDIRECTORY server data source, and a flat file data source.

Davis, however, teaches the identity integration system accomplishes a password update on at least one of an ACTIVE DIRECTORY data source, a SUN ONE server data source, a LOTUS NOTES server data source, a WINDOWS NT server data source, a NOVELL EDIRECTORY server data source, and a flat file data source as web server such as the Sun Web Server (col. 5 lines 25-27), Novell (col. 6 lines 11-16), and a database using a flat file technique (col. 7, lines 8-10) may be used.

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the teaching of Davis would have provided the combination of Hu/Bush's system with tools and technology that software developers can use to manage the environment of a computer system (col. 1 lines 57-63, Davis).

Response to Arguments

Applicant's arguments filed 2/14/2007 have been fully considered but they are not persuasive.

Claim 1 rejection

With respect to the rejection of claim 1, Applicant argues on page 25 of the response that Hu fails to teach the feature of "a management agent for each of the multiple data sources configured specifically for its respective data source..." The Examiner respectfully disagrees given the following:

Hu teaches a password management module 108 contained in server computer 104 (figure 1). Hu's password management module 108 can easily suggest the claimed management agent as this component provides password management activities (see 0035). Furthermore, the password management module identifies the target computer being accessed, retrieves the password from database 120 and then accesses the target computer with the password (0035). Therefore, password management module sufficiently describes the claimed management agent as it manages communication with at least one of the target computers. Furthermore, it can be seen that Hu's management module is essentially configured for its respective data source (i.e. target computer).

Further yet, Hu's password management module 108 contains log-in procedures for each target computer (also describing a management agent for each of the multiple data sources configured specifically for its respective data source). In other words, it is

inherent that the log-in scripts are configured specifically for its respective data source because Hu's log-in scripts are specific to each target computer (Hu, 0032).

Applicant further argues with respect to claim 1 on page 25 that Hu fails to teach the feature of custom logic configured as code. The Examiner respectfully disagrees given the following:

Hu teaches in [0037] that a user may specify particular computers for automatic log-in processing. A list of target URL's that require password access is provided so the user can accomplish this. A user therein suggests the custom logic source, with the custom logic being the specifying of the target computers for a log-in process. Further, as Hu teaches the log-in procedure is a script (e.g. 0010), it is sufficiently taught that the custom logic (specified target computers for automatic log- in) provided from the user is configured as code.

Applicant then argues with respect to claim 1 on page 25 and bottom of pages 26 and 27 of the remarks that Hu fails to teach performing a password operation on a password associated with at least one of the selected multiple data sources."

The Examiner disagrees because as a reasonably interpreted, one of skill in the art would believe that retrieving a password for the target computer (paragraph 0038) would easily suggest a password operation. Even more so, Hu's password management system (abstract) of managing passwords sufficiently teaches performing password operations because it effectively accesses and manages user's passwords

for accessing a target website. Also, Hu teaches a user can modify a password for each account [0067], which further anticipates a password operation on a password associated with each of the selected multiple data sources..." as recited in claim 1.

Claims 2-11 and 15-52

These claims are respectfully rejected as for depending upon rejected claim 1. Applicant's arguments to claim 1 have been found unpersuasive as seen in the response thereto above.

Claim 53 rejection

With respect to claim 53, applicant further argues that Hu does not disclose "custom logic conformed as code" and "request an update of a password associated with each designated account." With respect to the former argument, the Examiner respectfully submits that this argument is addressed in the response to arguments pertaining to claim 1.

With further respect to the latter argument of Hu not disclosing "request an update of a password associated with each designated account," the Examiner disagrees because in paragraph 0067, Hu teaches a displaying of various managed accounts, which allow the user to at least *modify* a password for *each* account (emphasis added). The Examiner respectfully submits that one of skill in the art would understandable acknowledge that at least modifying a password would include an update to the password (i.e. modifying is essentially the same as updating a password).

Claims 54-60

These claims are respectfully rejected as for depending upon rejected claim 53. Applicant's arguments to claim 53 have been found unpersuasive as seen in the response thereto above.

Claim 61

The Applicant argues (page 30 of the response) that Hu fails to teach the element of custom logic "configured as code." The Examiner disagrees as per the explanation of the response to arguments to claim 1.

Claims 62-64

These claims are respectfully rejected as for depending upon rejected claim 61. Applicant's arguments to claim 61 have been found unpersuasive as seen in the response thereto above.

Claim 65

With respect to claim 65, Applicant argues (page 32 of the response) that Hu does not disclose, "a management agent...configured to call for custom code from a custom logic source outside the identity integration system." The Examiner respectfully disagrees because Hu discloses a management agent (124, 118, 108, 0032, and 0035). Hu further teaches providing a list of target URL's so that the user (suggesting a custom logic source) can specify particular target computers for automatic log-in (a log-in

procedure suggests custom code as it is essentially "customized" for each target computer; see also beginning of 0034) processing and password access.

With further arguments to claim 65 that Hu fails to disclose "update passwords on each of the accounts based on the input password," the Examiner respectfully submits this limitation is addressed in the rejection above and further in response to the argument of claim 1.

Claims 66-73

These claims are respectfully rejected as for depending upon rejected claim 65. Applicant's arguments to claim 65 have been found unpersuasive as seen in the response thereto above.

Claim 74

The Applicant argues (page 33 of the response) that Hu fails to teach the element of custom logic "configured as code." The Examiner disagrees as per the explanation of the response to arguments to claims 1 and 65.

Claims 75-79

These claims are respectfully rejected as for depending upon rejected claim 74. Applicant's arguments to claim 74 have been found unpersuasive as seen in the response thereto above.

Claim 80

With respect to claim 80, Applicant argues (page 34 of the response) that Hu does not disclose "a management agent for each of multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source."

The Examiner respectfully disagrees because Hu teaches a password management module 108 with in the server 104 that communicates with target computers (112, 114, and 116). It is respectfully submitted that the module 108 is configured for at least a target computer (e.g. 113) as it retrieves a password from database 120 to access it (see 0034). Furthermore, Hu teaches a log-in script specific to each computer [0033]. This also suggests the claimed "a management agent for each of multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source" because a log-in script suggests, under a broad interpretation, that it can be an agent configured for its respective data source (i.e. target computer 112).

Also with respect to claim 80, Applicant argues that Hu does not disclose "allowing input of a request to update old passwords associated with each of the selected accounts to the new password input via the user interface." The Examiner respectfully disagrees because Hu teaches displaying various accounts (i.e. user interface) and providing sub-displays allowing the user to define and *modify* (i.e.

updating old passwords) password and account identifier information for each account (see also Fig. 7A and [0067]).

Claims 81-85

These claims are respectfully rejected as for depending upon rejected claim 80. Applicant's arguments to claim 80 have been found unpersuasive as seen in the response thereto above.

Conclusion

The Examiner respectfully submits that the arguments presented in the remarks filed 2/14/2007 have not been found to be persuasive as seen in the rejection above. Therefore, the rejection is maintained. Further arguments not addressed in this Action are rendered moot in view of Applicant's amendments necessitating new grounds of rejection.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert M. Timblin whose telephone number is 571-272-5627. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jean R. Homere can be reached on 571-272-3780. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Robert M. Timblin
Patent Examiner: AU 2167
5/16/2007

JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100